



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 03/29/2010
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER

ZECHER, CORDELIA P K

ART UNIT	PAPER NUMBER
----------	--------------

2432

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

03/29/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No. 10/752,420	Applicant(s) ROSE ET AL.	
	Examiner Cordelia Zecher	Art Unit 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 January 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-24, 26-28, 50, 51 and 53-56 is/are pending in the application.
- 4a) Of the above claim(s) 52 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5-24, 26-28, 50, 51 and 53-56 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed January 9, 2010 have been fully considered but they are not persuasive. Applicant argues that the recitation of a mobile user device in claim 14, overcomes the 101 rejection. However, as stated in previous office actions, even though the claims recite a device, there is no specific hardware recited in the claims. Since the specification defines that there are embodiments that include software only (page 6, paragraph 64), the claims are drawn to include software only embodiments. Applicant goes on to argue that further in the same paragraph the software MAY be stored in computer readable medium. However, this embodiment is in the alternative and does not overcome the 101 requirement. Therefore claims 14 – 21 are non-statutory. However, if the claims were amended to include hardware, such as a memory or display, then the claims would be statutory under 101.

2. Applicant argues that Lewis in view of Sudia fails to teach output of one private key, while retaining another private key. However, Lewis teaches that the first private key is put in one storage, and the second private key is put in a second storage which is physically separate from the main storage (column 6, lines 31-35). Therefore Lewis teaches retaining one key while moving another key to a different location. Sudia is cited for teaching splitting the key into shares before being outputted (column 18, lines 12-14). Therefore in combination Lewis in view of Sudia teaches retaining one key, while outputting a second key, and outputting the second key as a plurality of shares.

Art Unit: 2432

3. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would be desirable to split the users private key among several agents to enhance user and public trust in the system (column 20, line 66-column 21, line 4).

4. Applicant argues that there is no reasonable expectation of success in modifying the teachings of Lewis and Sudia to arrive at the limitations of claim 1. However, as stated above, Lewis teaches retaining one key, while outputting a second key (column 6, lines 31-35). Sudia teaches splitting a private key into key splits that are shared among a plurality of users (column 18, lines 12-14). One of ordinary skill in the art would be motivated to combine Lewis with Sudia to arrive at the invention of claim 1 because it is desirable to split the users private key among several agents to enhance user and public trust in the system (column 20, line 66-column 21, line 4).

5. Applicant argues that Lewis in view of Sudia fails to teach preventing retransmission of the second private key. However, Sudia teaches preventing replaying a rekey instruction (column 42, lines 14-19). Since the private key is only outputted when it is rekeyed, Sudia teaches preventing retransmission of the second private key. In addition, Lewis teaches outputting the key only once (column 10, lines 4-5).

6. Applicant argues that Lewis fails to teach or suggest using the second public key for authentication of the mobile user device if the first public key fails. Applicant argues that Lewis teaches that the message is authenticated using the Apu and therefore if the public key fails, that it could not be replaced. However, Lewis teaches that the key replacement message does not necessarily require the public key Apu and can instead use the public key of the node to encrypt the message since there is a chance the Apu has been compromised (column 10, lines 20-23). Therefore Lewis teaches using the second public key for authentication of the device if the first public key fails.

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 101

8. Claims 14 – 21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In the specification applicant defines the means to include software only [0064].

Claim Rejections - 35 USC § 103

9. Claims 1 – 3, 5 – 24, 26 – 28, 50,51 and 53 – 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis's US Patent 5,761,306, and further in view of Sudia US Patent 6,009,177. Referring to claims 1, 14 and 22, Lewis teaches:

- a. Creating a first private key and corresponding public key (column 6, lines 14-16).

Art Unit: 2432

- b. Creating a second private key associated with the first private key and creating a second public key corresponding to the second private key (column 6, lines 14-17).
 - c. Outputting the second private key while retaining the first private key (column 6, lines 31-35).
 - d. Disabling the first private key when the second private key is used (column 3, lines 25-26, and 61-62).
 - e. Transmitting the second public key concurrent with the first public key (column 3, lines 23-25, column 4, lines 12-14).
 - f. Using the first private key for authentication (column 8, lines 40-49).
10. Lewis fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

Art Unit: 2432

11. Referring to claims 2 and 23, Sudia teaches:

- g. Creating at least two shares of the second private key at the device (column 18, lines 12-14).
- h. Outputting each share to a different entity (column 18, lines 37-39).

12. Referring to claims 3, 16, and 24, Lewis teaches using the second private key for authentication (column 7, lines 31-37, column 8, lines 40-49). Sudia teaches re-creating the private key using the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

13. Referring to claims 5 and 17, Lewis teaches:

- i. Creating a third private key associated with the second private key, and creating a third public key corresponding to the third private key (column 7, lines 31-37).
- j. Outputting the third public key (column 7, lines 59-65).

14. Referring to claim 6, Lewis teaches using the third private key for authentication (column 7, lines 31-37, column 8, lines 40-49). Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). The suggestion/motivation for doing so would have been that it is desirable

Art Unit: 2432

to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

15. Referring to claim 7, Lewis teaches that the second private and public keys are created independently from the first private and public keys (column 7, lines 59-60).

16. Referring to claims 8 and 18, Lewis teaches:

k. Creating a third private key associated with the second key and creating a third public key corresponding to the third private key (column 7, lines 31-37).

l. Creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key (column 7, lines 31-37).

m. Outputting the third and fourth public keys (column 7, lines 59-65).

17. Lewis fails to teach outputting the fourth private key once such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

18. Referring to claim 9, Lewis teaches:

n. Disabling use of the second private key for authentication (column 3, lines 25-26).

o. Using the third private key for authentication (column 8, lines 40-49).

p. Using the fourth private key for authentication (column 8, lines 40-49).

Art Unit: 2432

19. Lewis fails to teach recreating the fourth private key. Sudia teaches re-creating the private key using the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

20. Referring to claim 10, Sudia teaches preventing retransmission of the second private key (column 42, lines 14-19).

21. Referring to claims 11, 19, and 26, Lewis discloses:

q. Receiving a first public key (column 10, lines 1-4).

r. Receiving a second public key concurrent with receipt of the first public key, the second public key associated with the first public key (column 10, lines 1-4), wherein the second public key has a corresponding second private key (column 6, lines 14-17), and the first private key is disabled when the second private key is recreated and used for authentication (column 3, lines 25-26, column 4, lines 12-14).

s. Using the first public key for authentication (column 8, lines 40-49).

t. Using the second public key for authentication if the first public key fails (column 8, lines 58-64).

Art Unit: 2432

22. Lewis fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

23. Referring to claims 12, 20 and 27, Lewis teaches receiving a third public key from the device, the third public key associated with the second public key (column 7, lines 31-37), if the first public key fails and the second key results in successful authentication (column 8, lines 58-64).

24. Referring to claims 13, 21, and 28, Lewis teaches a third public key and a fourth public key from the device (column 7, lines 31-37), if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second key (column 8, lines 58-64).

25. Referring to claim 15, Sudia teaches:

- u. Creating at least two shares of the private key (column 18, lines 12-14).

Art Unit: 2432

v. Wirelessly (column 26, line 65) outputting each share once to a different entity (column 18, lines 37-39), wherein subsequent outputting of the second private key is prevented (column 42, lines 14-19).

26. Referring to claim 50, Lewis teaches:

w. A processor configured to generate a first private key and corresponding first public key, the processor configured to generate a second private key associated with the first private key and to create a second public key corresponding to the second private key (column 6, lines 14-17).

x. A storage medium coupled to the processor to store the first private key (column 6, lines 14-17).

y. A transmitter to output the second public key to the device concurrent with outputting the first public key (column 10, lines 1-4) and disable the first private key when the second private key is created and used for authentication (column 3, lines 25-26, column 4, lines 12-14).

z. Wherein the processor uses the first private key for authentication of the device (column 8, lines 40-49).

27. Lewis fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the network communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted

Art Unit: 2432

communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

28. Referring to claim 51, Lewis teaches:

aa. A receiver configured to receive a first public key from a device and receiving a second public key from the device concurrent with receipt of the first public key, the second public key associated with the first public key (column 10, lines 1-4), wherein the second public key has a corresponding second private key (column 6, lines 14-17), and the first private key is disabled when the second private key is recreated and used for authentication (column 3, lines 25-26, column 4, lines 12-14).

bb. A storage medium coupled to the receiver configured to store the first and second public keys (column 10, lines 1-4).

cc. A processor coupled to the receiver, the processor configured to use the first public key for authentication (column 8, lines 40-49), the processor configured to use the second public key for authentication if the first public key fails (column 8, lines 58-64).

29. Lewis fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches

Art Unit: 2432

breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

30. Referring to claims 53 – 56, Lewis teaches the second private key is removed from the user device upon transmission of the second private key (column 6, lines 31-35).

31. Lewis fails to teach a wirelessly transmission of a plurality of shares of the private key. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key

Art Unit: 2432

split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

Conclusion

32. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Zecher whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2432

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. Z./

Examiner, Art Unit 2432

/Benjamin E Lanier/

Primary Examiner, Art Unit 2432